RSAC 2025 Conference

Many Voices.
One Community.

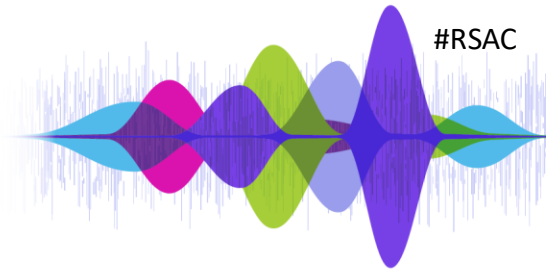
SESSION ID: LAB2-W08

What Just Happened?! How Traffic Distribution Systems Fool Everyone

Brent Eskridge, PhD
Staff Threat Researcher
Infoblox
linkedin.com/in/brenteskridge/

Christopher Kim
Senior Staff Threat Researcher
Infoblox
linkedin.com/in/christopherk/

Dave Mitchell
Principal Threat Researcher
Infoblo
linkedin.com/in/mitchelldavex



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

WARNING

The ads and content in malicious traffic distribution systems (TDSs), and malicious adtech in general, are out of our control and you may encounter explicit content while hunting. However, if you encounter illegal content, such as that including minors or the harm of an individual, please notify us immediately.

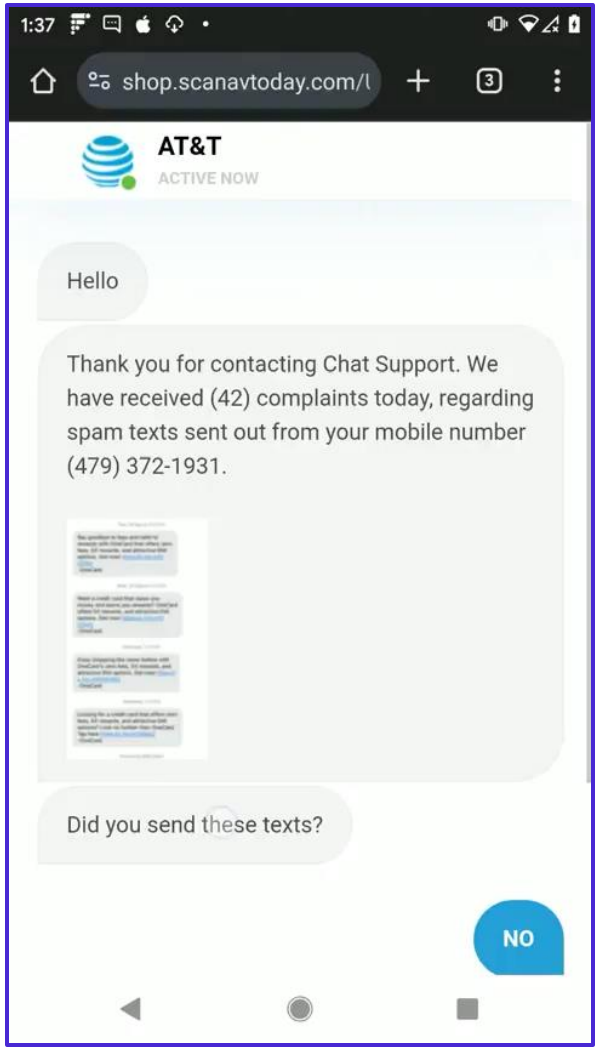
RSAC 2025 Conference

Experience a Traffic Distribution System (TDS) Firsthand

Interactive Lab

Many Voices.
One Community.

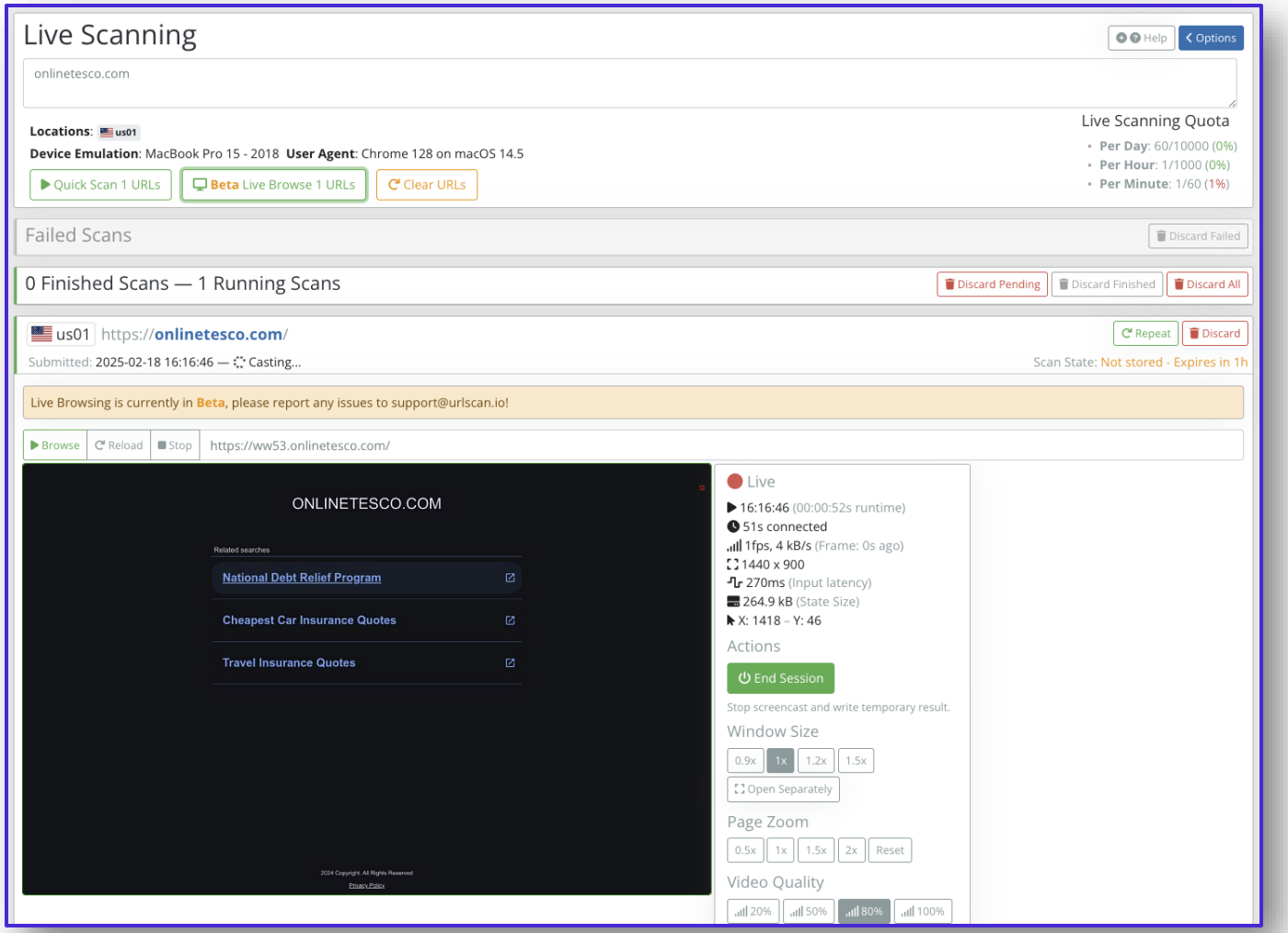
Malicious TDSs In the Wild


1:37
shop.scanavtoday.com/t
AT&T
ACTIVE NOW
Hello
Thank you for contacting Chat Support. We have received (42) complaints today, regarding spam texts sent out from your mobile number (479) 372-1931.
Did you send these texts?
NO

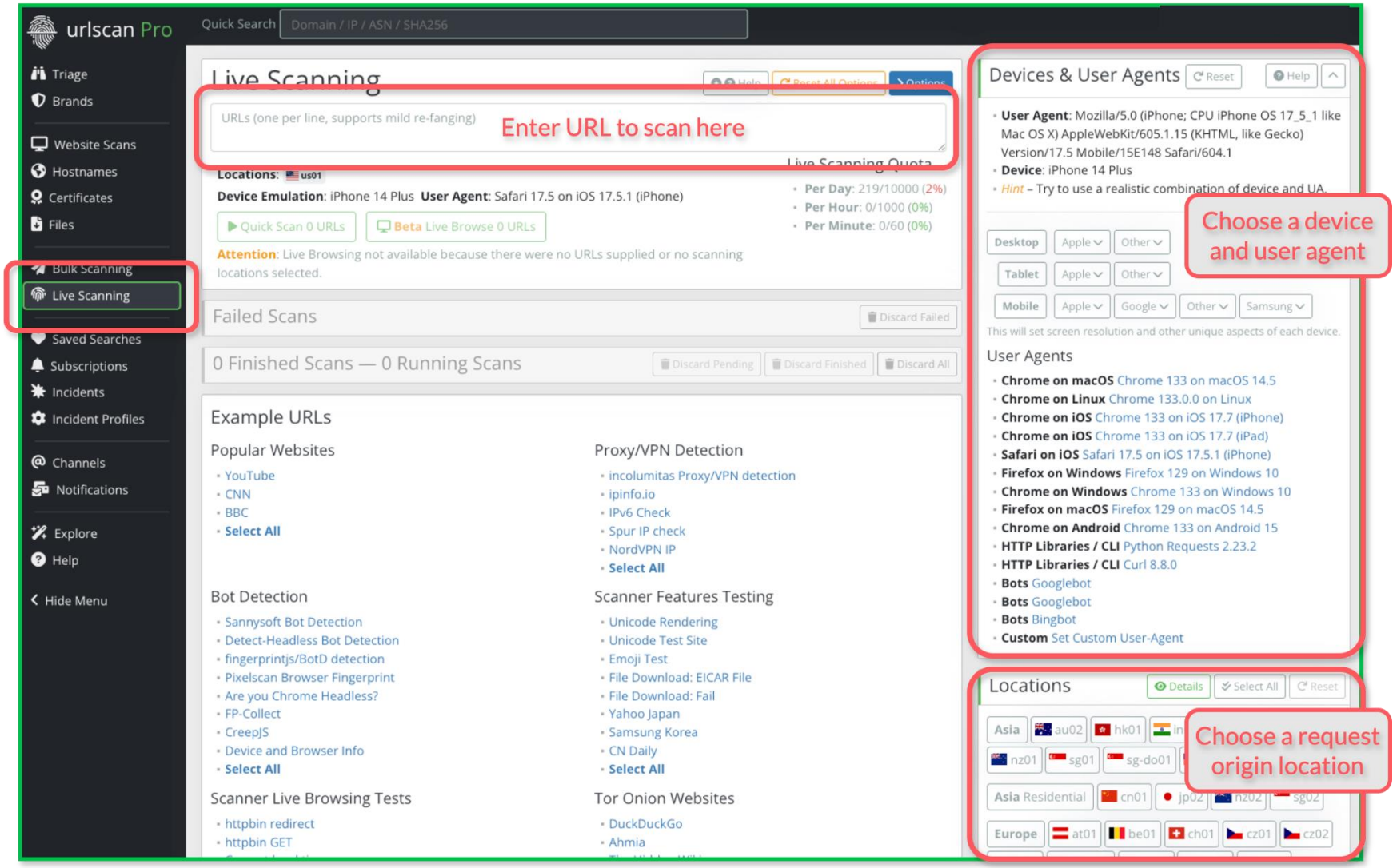
AT&T scareware scam

Compromised domain with suspicious VPN

TDS Live Example



Now It Is Your Turn



RSAC 2025 Conference

What is a TDS?

Discussion

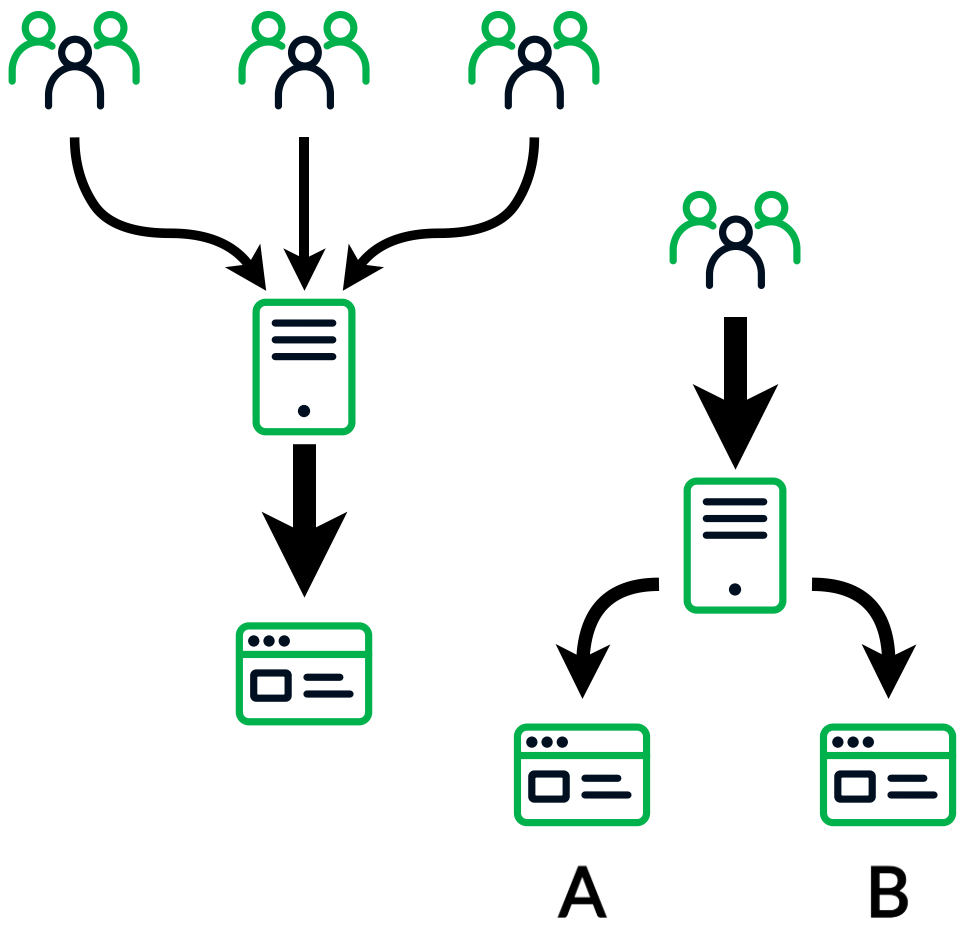
Many Voices.
One Community.

Traffic Distribution System (TDS)

- Filters incoming traffic and redirects it to another location
- Easier to direct large volumes of traffic to multiple destinations
- Many legitimate TDS services exist (e.g., Keitaro)
- AKA “Traffic Delivery System”

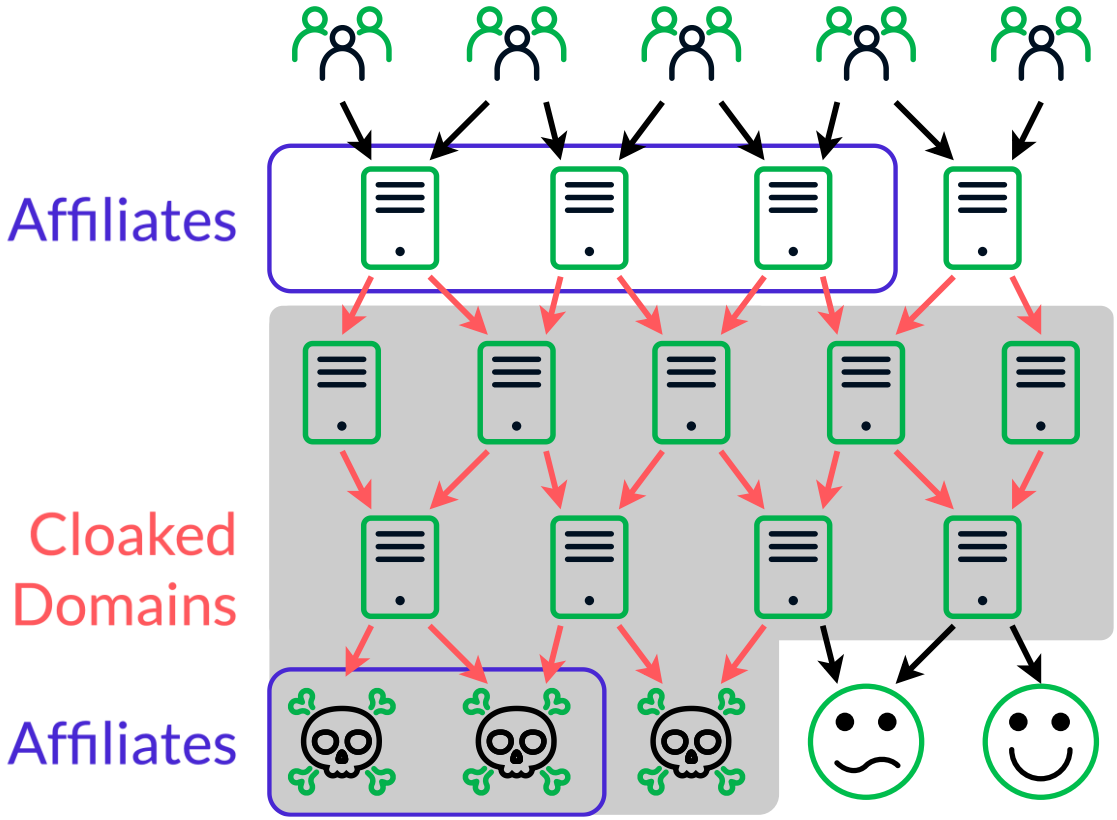
Traffic Distribution System (TDS) *cont'd*

- Initially developed for affiliate marketing
- Key uses
  - Manage traffic flow between different content
  - A/B Testing
  - Prevent bots from skewing results (and therefore, payouts)



Value of TDSs to Threat Actors

- Infrastructure and landing pages are cloaked to evade detection
- Affiliates increase traffic to TDS
- Affiliates purchase traffic for landing pages
- TDS sends undesirable traffic to decoy pages or legitimate sites



TDS Threat Delivery: Corporate

- Many of the threats delivered by TDSs steal victim's information
- Delivered malware is usually an infostealer
  - Most prevalent malware in 2023 (Link)
- Infostealers are at the heart of corporate data breaches
  - Snowflake attacks (Link)
  - AU government report (Link)
  - Trends analysis (Link)

TDS Threat Delivery: Consumer

- Design allows for a variety of threats active in the same network at the same time
- Threats target specific victim profiles
  - Operating System
  - Platform (e.g., desktop vs. mobile)
  - Geographic region
- TDS routes victims to appropriate threat
- Difficult for users to break out of the TDS once inside

Threats Delivered By Malicious TDSs

DNS Threat Actor	Infostealer	Scam	Phishing	Domain Hijacking
Vacant Viper	✓	✓		✓
Vane Viper	✓			
Vextrio Viper	✓	✓	✓	✓
Hasty Hawk			✓	
Sophisticated Chickens			✓	✓
BlackTDS	✓		✓	
Parrot TDS	✓			
R0bl0ch0n TDS		✓		

How Big are Malicious TDS Networks?

Network	Domains
Vigorish Viper	443K
Vigorish Viper Affiliate Tianbo	138K
VexTrio Viper	88K
Undisclosed SMS Scam TDS	63K
Vane Viper	37K
Undisclosed CNAME Malware TDS	19K
Venal Viper	18K

Domain counts are approximate and do not include affiliates

RSAC 2025 Conference

Investigating TDS Domains

Interactive Lab

Many Voices.
One Community.

Top 10 Ways to Identify Malicious Adtech

1. Different landing pages when using different devices, locations, etc.
2. Redirections through multiple sites
3. Landing on a popular website
4. Pages with fake captchas
5. Push notification request immediately upon landing at a weird location or domain

Top 10 Ways to Identify Malicious Adtech *(cont'd)*

6. Pages with suspicious scripts
7. URLs that include terms like tracker, smartlink, checker, or zeroclick
8. Resolutions to a large number of ASNs, usually with a combination of Cloudflare, dedicated services, Russian, or small ASN hosting
9. Victim data collection via URL parameters and antibot services
10. Single page websites

URLScan Examples

- Different landing pages when using different devices, locations, etc.
  - VPN Cloaking: Scareware (Link), Fake parking (Link), Legit domain redirect (Link)
  - Compromised Domain: Bing redirect (Link), Survey Scam (Link)
- Redirections through multiple sites
  - Vextrio Viper (Link)
  - Fake News (Link)

URLScan Examples *(cont'd)*

- Landing on a popular website
  - ZeroClick landing at Banggood (Link)
  - Vextrio Viper landing at Twitter/X (Link)
  - Vextrio Viper landing at GooglePlay (Link)

URLScan Examples *(cont'd)*

- Pages with fake captchas
  - Fake YouTube captcha (Link)
  - Robot captcha (Link)
  - Mobile SMS captcha (Link)
- Push notification request immediately upon landing at a weird location or domain
  - Allow notifications to watch a video (Link)

Identification Challenge

- Form teams of 2-3 people
- Using URLScan, classify as many domains from the list as you can in the given time
- Possible options
  - Yes, it is part of a TDS
  - No, it is not part of a TDS
  - Maybe?

URLScan Tips

- Use previous scans to find different results
- Different scan sizes may mean different content
- Scans will accept defanged domains, but searches require valid domains

Identification Challenge Reflection

- For each TDS domain you found:
  - Who does the TDS appear to target?
  - What threats does it pose?
  - How well was their infrastructure cloaked?
- Did you find any trends in the TDS domains?

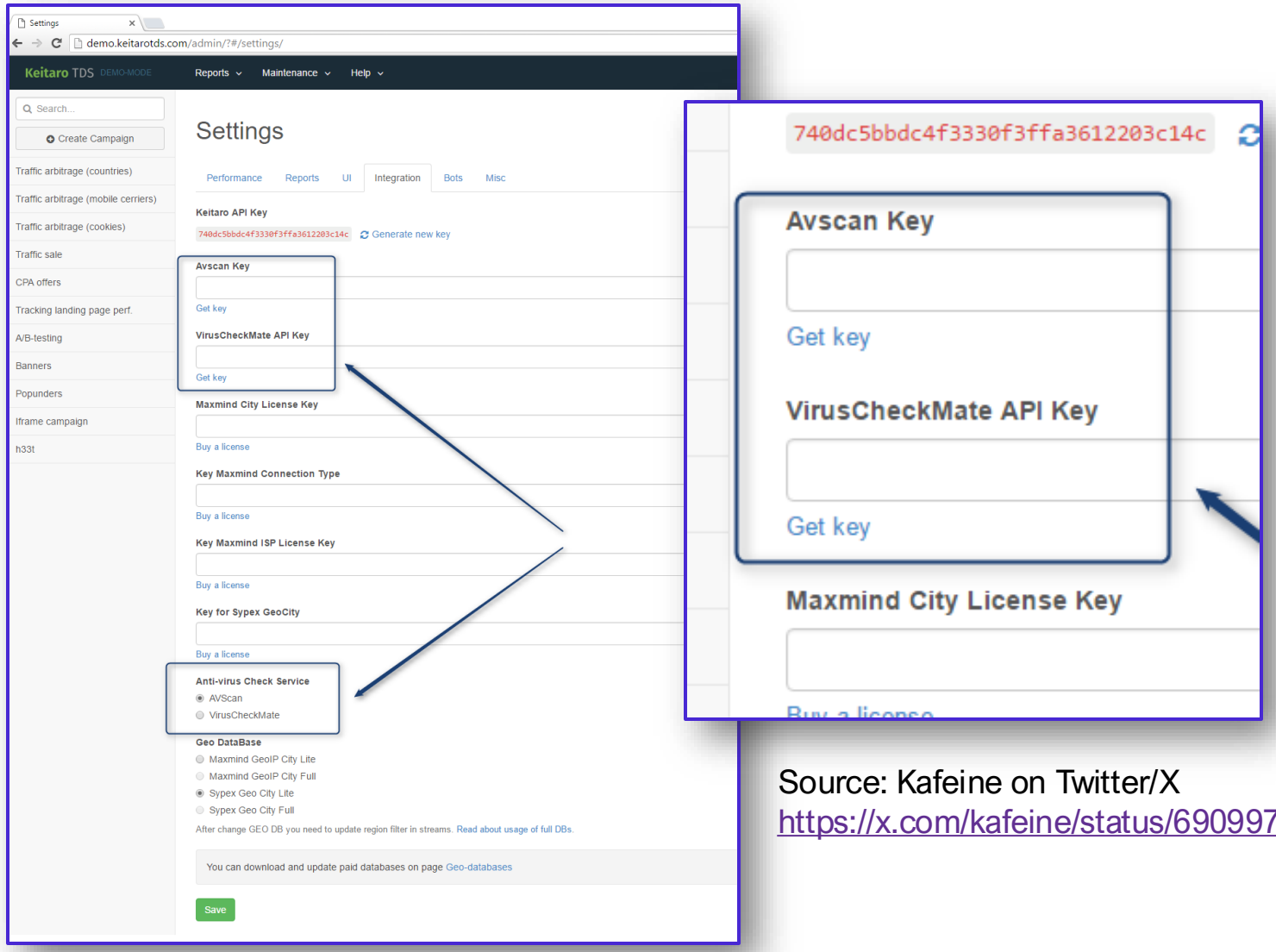
RSAC 2025 Conference

Operating a TDS

Demonstration

Many Voices.
One Community.

Adtech Management Example: Keitaro



Source: Kafeine on Twitter/X
https://x.com/kafeine/status/690997790118387712

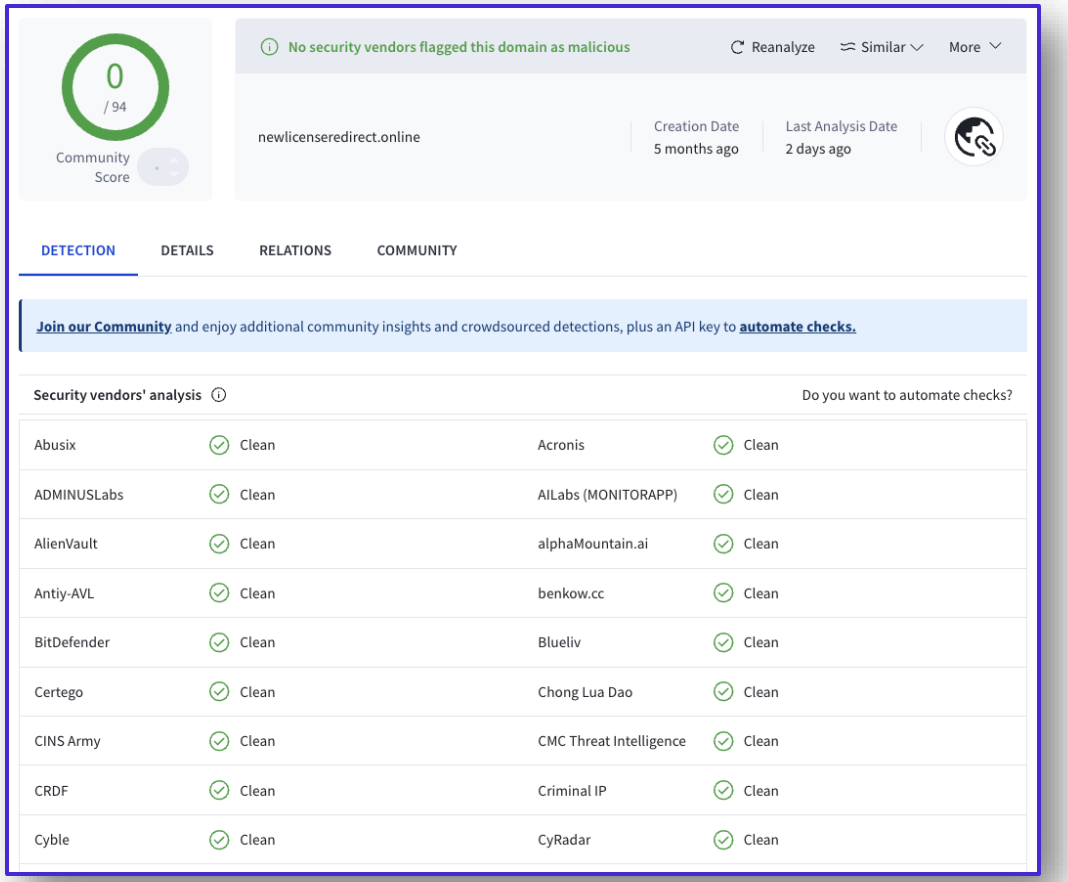
RSAC 2025 Conference

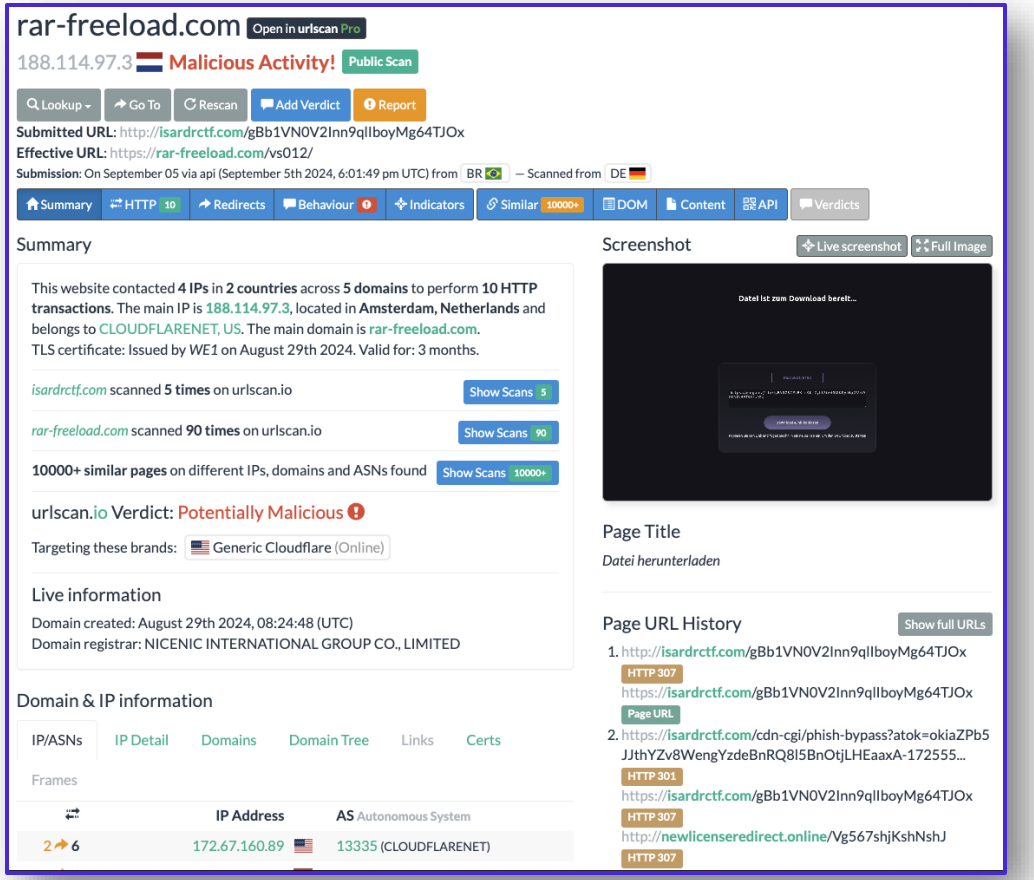
Defending Against a TDS

Demonstration

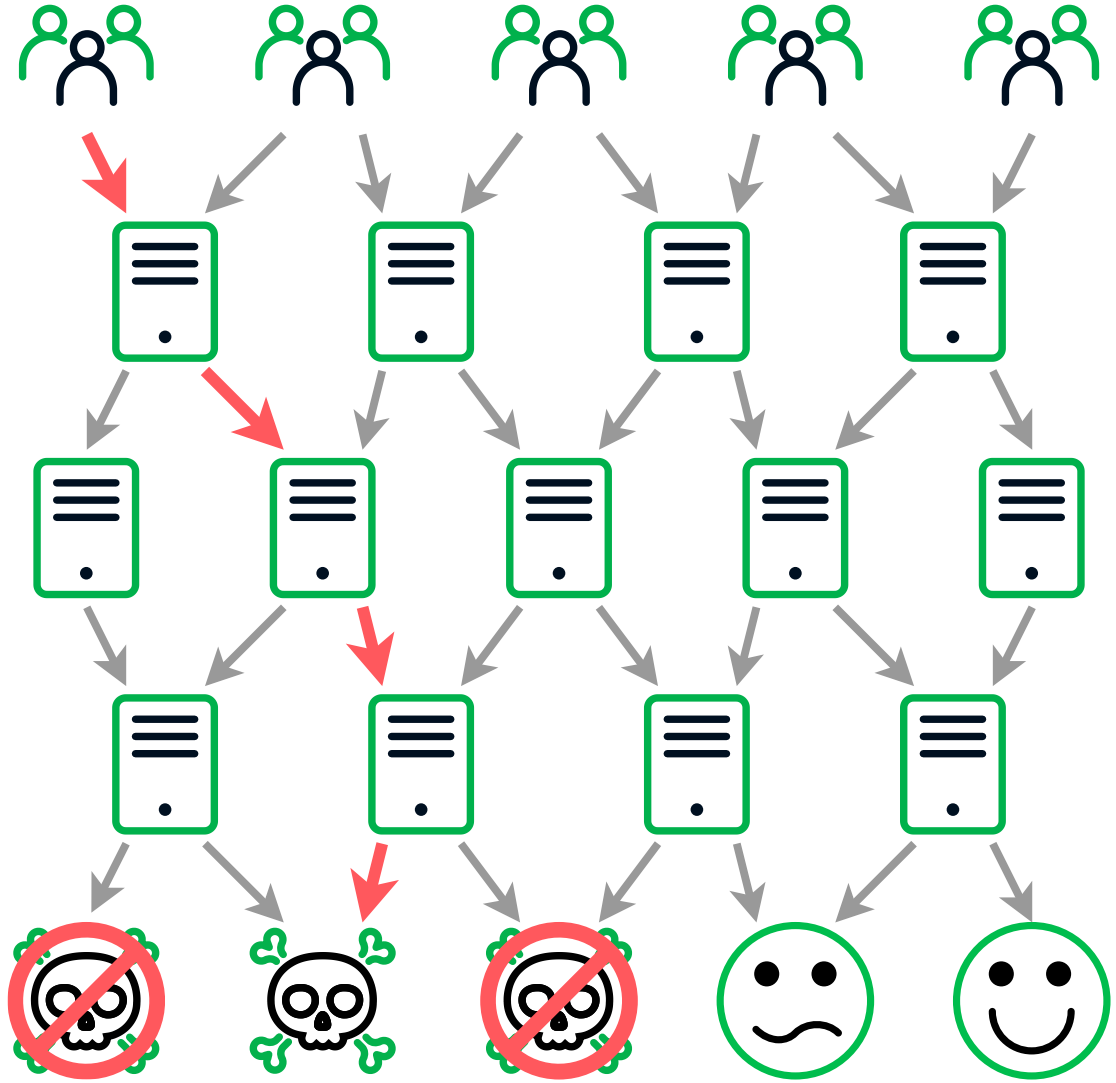
Many Voices.
One Community.

Underestimated Threats

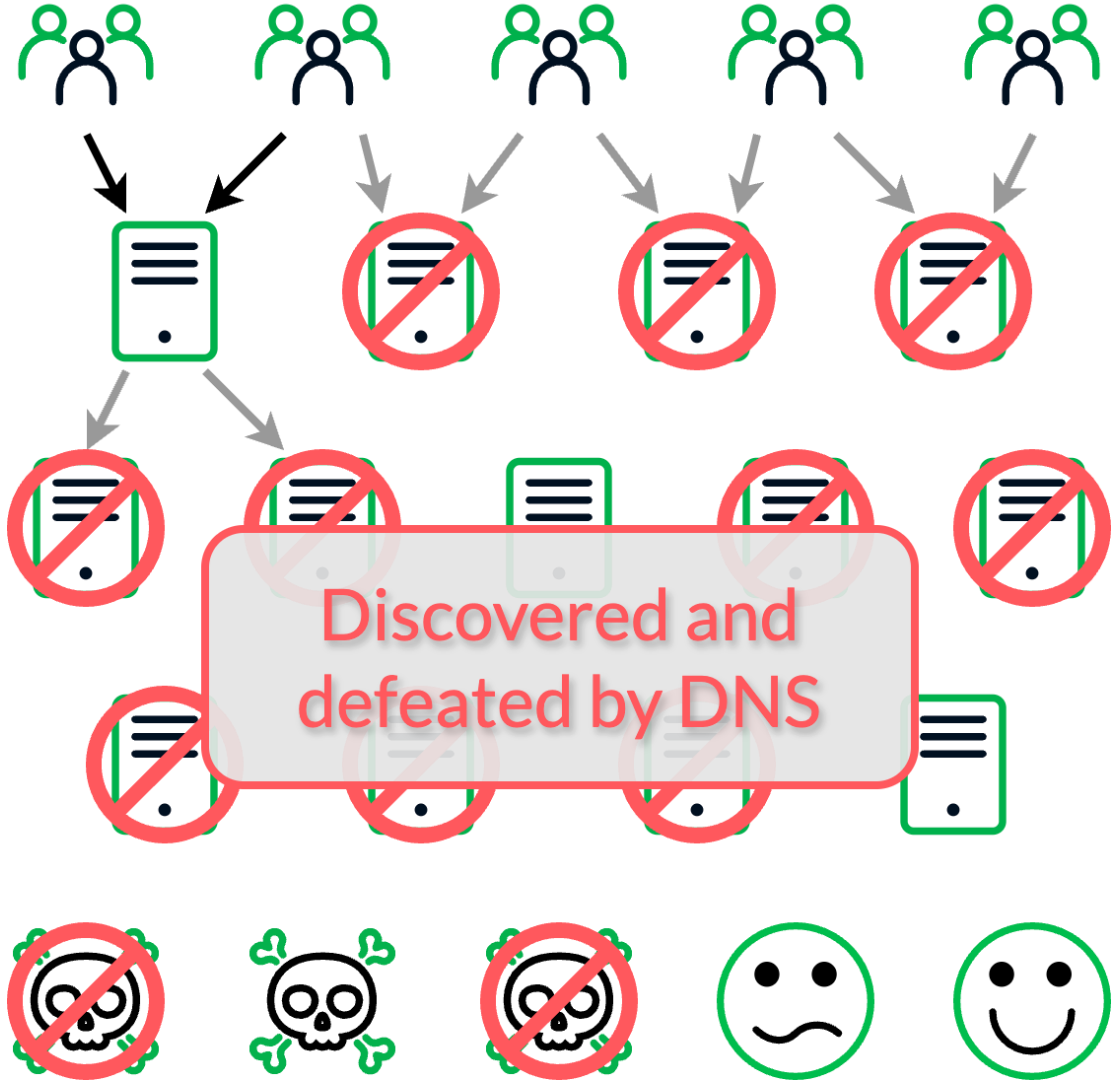




TDSs Are Resilient



DNS Is Essential in Defeating a TDS



Stopping TDSs Discussion

- What makes defending against a TDS challenging?
  - Technological challenges
  - Business challenges
- How would you find out if a threat is part of a TDS?
- How would you hunt for a new TDS before you see it in your network?

RSAC™ 2025 Conference

So Where Do You Go From Here?

Don’t Be Fooled! Apply What You Learned Today

- TDSs cloak their infrastructure and are everywhere
  - Don’t believe what you see
  - Use DNS to look deeper
  - Numerous free and paid tools to look beyond the landing page
- Blocking malicious landing pages doesn’t work long term
  - TDSs are resilient and adaptive
  - Use DNS to find and block their entire infrastructure

Resource Links

- Our Threat Intel Publications
  https://www.infoblox.com/threat-intel/
- Infoblox Threat Intel public IoC GitHub repository
  https://github.com/infobloxopen/threat-intelligence
- URLScan
  https://urlscan.io

RSAC 2025 Conference

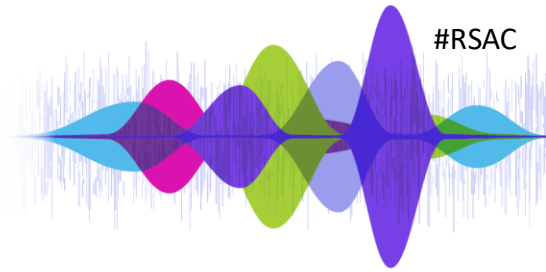
Many Voices.
One Community.

Infoblox
Threat Intel

Thank You!

Talk to us on Mastodon

infobloxthreatintel@infosec.exchange



References

- Pushed Down the Rabbit Hole *(Infoblox Threat Intel)*
- Click Bait and Switch: Malicious Traffic Distribution Systems *(Infoblox Threat Intel)*
- Cybercrime Central: VexTrio Operates Massive Criminal Affiliate Program *(Infoblox Threat Intel)*
- An Update on Fake Updates: Two New Actors, and New Mac Malware *(Proofpoint)*
- Why the Keitaro TDS keeps causing security headaches *(TechTarget)*
- A year in the cybersecurity trenches with Mandiant Managed Defense *(Mandiant)*
- UNC5537 Targets Snowflake Customer Instances for Data Theft and Extortion *(Mandiant)*
- The silent heist: cybercriminals use information stealer malware to compromise corporate networks *(Australian Government)*
- Breached Identities and Infostealers: One of the Largest Ongoing Data Leaks in History *(Flare)*

RSAC 2025 Conference

Questions?